

T S5/5/1

5/5/1

DIALOG(R)File 351:Derwent WPI

(c) 2005 Thomson Derwent. All rts. reserv.

013608276

WPI Acc No: 2001-092484/200111

XRPX Acc No: N01-069981

**Electronic storage device for guaranteeing originality of electronic data
varies level of access based on if data are original data or not**

Patent Assignee: RICOH KK (RICO)

Inventor: KANAI Y; YACHIDA M

Number of Countries: 002 Number of Patents: 007

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
DE 10024753	A1	20001221	DE 1024753	A	20000519	200111 B
JP 2000339223	A	20001208	JP 99145340	A	19990525	200113
JP 2001005728	A	20010112	JP 99173371	A	19990618	200118
JP 2001147898	A	20010529	JP 99328802	A	19991118	200136
JP 2001154577	A	20010608	JP 99338741	A	19991129	200138
JP 2001209582	A	20010803	JP 200015092	A	20000124	200150
JP 2001209581	A	20010803	JP 200015091	A	20000124	200150

Priority Applications (No Type Date): JP 200015092 A 20000124; JP 99145340
A 19990525; JP 99173371 A 19990618; JP 99328802 A 19991118; JP 99338741 A
19991129; JP 200015091 A 20000124

Patent Details:

Patent No	Kind	Lan Pg	Main IPC	Filing Notes
DE 10024753	A1	159	G06F-012/14	
JP 2000339223	A	29	G06F-012/14	
JP 2001005728	A	46	G06F-012/14	
JP 2001147898	A	11	G06F-015/00	
JP 2001154577	A	12	G09C-001/00	
JP 2001209582	A	18	G06F-012/14	
JP 2001209581	A	16	G06F-012/14	

Abstract (Basic): DE 10024753 A1

NOVELTY - The storage device includes a storage unit which stores electronic data consisting of a number of content files as a single original in an identifiable state. An access unit controls the access to the original electronic data at a level which is different from the level of access to non-original electronic data. The storage unit stores tamper detection information as original information corresponding to the electronic data.

DETAILED DESCRIPTION - The storage device may include a tamper detection information computing device which receives a request to re-store the electronic data as a single original using an encryption key to compute tamper detection information for each of the content files. A second tamper detection information computing device uses the encryption key to compute second temper detection information for edition management information. **INDEPENDENT CLAIMS** are included for an electronic storage device, an authorization verification system, an electronic storage method, an authorization verification method, damage recovery method and a storage medium for storing a program in a computer.

USE - For originality-guarantee electronic preservation systems using large-capacity storage media.

ADVANTAGE - Allows the originality of a combined document comprising multiple files to be guaranteed.

pp; 159 DwgNo 0/74

Title Terms: ELECTRONIC; STORAGE; DEVICE; GUARANTEE; ELECTRONIC; DATA; VARY
; LEVEL; ACCESS; BASED; DATA; ORIGINAL; DATA

Derwent Class: P85; T01

International Patent Class (Main): G06F-012/14; G06F-015/00

International Patent Class (Additional): G06F-003/06; G06F-009/06;
G06F-012/00; G06F-012/16; G06F-017/30; G06F-017/60; G09C-001/00

File Segment: EPI; EngPI

?

【特許請求の範囲】

【請求項1】 電子データを記憶する大容量記憶媒体および暗号鍵などを記憶する内部記憶媒体を少なくとも有し、前記電子データの原本性を保証する原本性保証電子保存装置において、

前記大容量記憶媒体に保存するファイルのリストを示すファイルリストを暗号化した署名情報並びに該大容量記憶媒体の媒体識別情報に基づいて前記大容量記憶媒体の正当性を検証することを特徴とする原本性保証電子保存装置。

【請求項2】 前記大容量記憶媒体に保存する保存ファイルのリストを示すファイルリストのハッシュ値を暗号化したリスト署名と、前記大容量記憶媒体の媒体識別情報とを対応づけた媒体認証コードリストを作成する媒体認証コードリスト作成手段と、

前記媒体認証コードリスト作成手段により作成された媒体認証コードリストに基づいて前記大容量記憶媒体の正当性を検証する正当性検証手段と、

を備えたことを特徴とする請求項1に記載の原本性保証電子保存装置。

【請求項3】 前記媒体認証コードリスト作成手段により作成された媒体認証コードリストを前記内部記憶媒体に格納し、前記大容量記憶媒体を装置本体に装着する際に、前記内部記憶媒体に格納された媒体認証コードリストに基づいて前記大容量記憶媒体の正当性を検証することを特徴とする請求項2に記載の原本性保証電子保存装置。

【請求項4】 暗号鍵などを記憶する内部記憶媒体を用いて大容量記憶媒体に記憶した電子データの原本性を保証する原本性保証電子保存方法において、

前記大容量記憶媒体に保存するファイルのリストを示すファイルリストを暗号化した署名情報並びに該大容量記憶媒体の媒体識別情報に基づいて前記大容量記憶媒体の正当性を検証することを特徴とする原本性保証電子保存方法。

【請求項5】 前記大容量記憶媒体に保存する保存ファイルのリストを示すファイルリストのハッシュ値を暗号化したリスト署名と、前記大容量記憶媒体の媒体識別情報とを対応づけた媒体認証コードリストを作成する媒体認証コードリスト作成工程と、

前記媒体認証コードリスト作成工程により作成された媒体認証コードリストに基づいて前記大容量記憶媒体の正当性を検証する正当性検証工程と、

を含んだことを特徴とする請求項4に記載の原本性保証電子保存方法。

【請求項6】 前記媒体認証コードリスト作成工程により作成された媒体認証コードリストを前記内部記憶媒体に格納し、前記大容量記憶媒体を装置本体に装着する際に、前記内部記憶媒体に格納された媒体認証コードリストに基づいて前記大容量記憶媒体の正当性を検証するこ

とを特徴とする請求項5に記載の原本性保証電子保存方法。

【請求項7】 前記請求項3～6のいずれか一つに記載された方法をコンピュータに実行させるプログラムを記録したことを特徴とするコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、電子データを記憶する大容量記憶媒体および暗号鍵などを記憶する内部記憶媒体を少なくとも有し、前記電子データの原本性を保証する原本性保証電子保存装置、原本性保証電子保存方法および記録媒体に関し、特に、大容量記憶媒体の状態を過去の状態に戻すというような大容量記憶媒体の不正なすり替えを効率良く防止することができる原本性保証電子保存装置、原本性保証電子保存方法および記録媒体に関する。

【0002】

【従来の技術】近年のコンピュータ技術の進展に伴うペーパーレス化の進展に伴って、紙によって原本書類として保存されていた情報が電子データの形式で保存される場合が増えてきたため、かかる電子データの原本性を保証する従来技術が知られている。

【0003】たとえば、「金井他：原本性保証電子保存システムの開発—システムの構築—, Medical Imaging Technology, Vol.16, No.4, Proceedings of JAMIT Annual Meeting'98(1998)」や、「国分他：原本性保証電子保存システムの開発, (特)情報処理振興事業協会発行 創造的ソフトウェア育成事業およびエレクトロニック・コマース推進事業 最終成果発表会論文集 創造的ソフトウェア育成事業編(1998)」には、電子データの原本性を保証するシステムの一例が開示されている。

【0004】かかる従来技術を用いると、電子データの原本性を保証することが可能となり、これにより原本書類を電子データの形式で保存し、もって高度情報化社会の推進並びに社会全体の生産性向上に寄与することができる。

【0005】

【発明が解決しようとする課題】しかしながら、これらの従来技術では、各ファイルのデータにメッセージ認証子を付加することでファイルの改ざんを検知しているため、たとえば大容量記憶媒体の状態を過去の状態に戻すというような大容量記憶媒体の不正なすり替えがおこなわれた場合に対応できないという問題がある。

【0006】特に、たとえば大規模なペーパーレス化を図るような場合には、数多くの大容量記憶媒体を用いねばならず、いきおい第三者がこの大容量記憶媒体に係る不正なすり替えをおこなう得るケースが増加し、この大容量記憶媒体に係る不正なすり替えをいかに防止するか

【0007】この発明は、上記問題（課題）に鑑みてなされたものであり、大容量記憶媒体の状態を過去の状態に戻すというような大容量記憶媒体の不正なすり替えを効率良く防止することができる原本性保証電子保存装置、原本性保証電子保存方法および記録媒体を提供することを目的とする。

【0008】

【課題を解決するための手段】上記目的を達成するために、請求項1の発明に係る原本性保証電子保存装置は、電子データを記憶する大容量記憶媒体および暗号鍵などを記憶する内部記憶媒体を少なくとも有し、前記電子データの原本性を保証する原本性保証電子保存装置において、前記大容量記憶媒体に保存するファイルのリストを示すファイルリストを暗号化した署名情報並びに該大容量記憶媒体の媒体識別情報に基づいて前記大容量記憶媒体の正当性を検証することを特徴とする。

【0009】この請求項1の発明によれば、大容量記憶媒体に保存するファイルのリストを示すファイルリストを暗号化した署名情報並びに該大容量記憶媒体の媒体識別情報に基づいて大容量記憶媒体の正当性を検証することとしたので、大容量記憶媒体の状態を過去の状態に戻すというような大容量記憶媒体の不正なすり替えを効率良く防止することができる。

【0010】また、請求項2の発明に係る原本性保証電子保存装置は、前記大容量記憶媒体に保存する保存ファイルのリストを示すファイルリストのハッシュ値を暗号化したリスト署名と、前記大容量記憶媒体の媒体識別情報とを対応づけた媒体認証コードリストを作成する媒体認証コードリスト作成手段と、前記媒体認証コードリスト作成手段により作成された媒体認証コードリストに基づいて前記大容量記憶媒体の正当性を検証する正当性検証手段と、を備えたことを特徴とする。

【0011】この請求項2の発明によれば、大容量記憶媒体に保存する保存ファイルのリストを示すファイルリストのハッシュ値を暗号化したリスト署名と、大容量記憶媒体の媒体識別情報とを対応づけた媒体認証コードリストを作成し、作成した媒体認証コードリストに基づいて大容量記憶媒体の正当性を検証することとしたので、この媒体認証コードリストを用いて大容量記憶媒体の正当性を効率良く検証することができる。

【0012】また、請求項3の発明に係る原本性保証電子保存装置は、前記媒体認証コードリスト作成手段により作成された媒体認証コードリストを前記内部記憶媒体に格納し、前記大容量記憶媒体を装置本体に装着する際に、前記内部記憶媒体に格納された媒体認証コードリストに基づいて前記大容量記憶媒体の正当性を検証することを特徴とする。

【0013】この請求項3の発明によれば、媒体認証コードリストを前記内部記憶媒体に格納し、大容量記憶媒体を装置本体に装着する際に、この内部記憶媒体に格納

された媒体認証コードリストに基づいて大容量記憶媒体の正当性を検証することとしたので、内部記憶媒体を有効に利用して大容量記憶媒体の正当性を効率良く検証することができる。

【0014】また、請求項4の発明に係る原本性保証電子保存方法は、暗号鍵などを記憶する内部記憶媒体を用いて大容量記憶媒体に記憶した電子データの原本性を保証する原本性保証電子保存方法において、前記大容量記憶媒体に保存するファイルのリストを示すファイルリストを暗号化した署名情報並びに該大容量記憶媒体の媒体識別情報に基づいて前記大容量記憶媒体の正当性を検証することを特徴とする。

【0015】この請求項4の発明によれば、大容量記憶媒体に保存するファイルのリストを示すファイルリストを暗号化した署名情報並びに該大容量記憶媒体の媒体識別情報に基づいて大容量記憶媒体の正当性を検証することとしたので、大容量記憶媒体の状態を過去の状態に戻すというような大容量記憶媒体の不正なすり替えを効率良く防止することができる。

【0016】また、請求項5の発明に係る原本性保証電子保存方法は、前記大容量記憶媒体に保存する保存ファイルのリストを示すファイルリストのハッシュ値を暗号化したリスト署名と、前記大容量記憶媒体の媒体識別情報とを対応づけた媒体認証コードリストを作成する媒体認証コードリスト作成工程と、前記媒体認証コードリスト作成工程により作成された媒体認証コードリストに基づいて前記大容量記憶媒体の正当性を検証する正当性検証工程と、を含んだことを特徴とする。

【0017】この請求項5の発明によれば、大容量記憶媒体に保存する保存ファイルのリストを示すファイルリストのハッシュ値を暗号化したリスト署名と、大容量記憶媒体の媒体識別情報とを対応づけた媒体認証コードリストを作成し、作成した媒体認証コードリストに基づいて大容量記憶媒体の正当性を検証することとしたので、この媒体認証コードリストを用いて大容量記憶媒体の正当性を効率良く検証することができる。

【0018】また、請求項6の発明に係る原本性保証電子保存方法は、前記媒体認証コードリスト作成工程により作成された媒体認証コードリストを前記内部記憶媒体に格納し、前記大容量記憶媒体を装置本体に装着する際に、前記内部記憶媒体に格納された媒体認証コードリストに基づいて前記大容量記憶媒体の正当性を検証することを特徴とする。

【0019】この請求項6の発明によれば、媒体認証コードリストを前記内部記憶媒体に格納し、大容量記憶媒体を装置本体に装着する際に、この内部記憶媒体に格納された媒体認証コードリストに基づいて大容量記憶媒体の正当性を検証することとしたので、内部記憶媒体を有効に利用して大容量記憶媒体の正当性を効率良く検証することができる。

【0020】また、請求項7の発明に係る記録媒体は、前記請求項3～6のいずれか一つに記載された方法をコンピュータに実行させるプログラムを記録したことで、そのプログラムが機械読み取り可能となり、これによって、請求項3～6の動作をコンピュータによって実現することができる。

【0021】

【発明の実施の形態】以下に添付図面を参照して、この発明に係る原本性保証電子保存方法およびその方法をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体の好適な実施の形態を詳細に説明する。

【0022】図1は、本実施の形態に係る原本性保証電子保存方法を実行する電子保存装置のブロック構成図である。ユーザは、ホスト計算機2側からネットワーク（単なる通信路で良い）を介して電子保存装置1に対して電子データの保存処理や読み出し処理を実行することができる。

【0023】図1に示す電子保存装置1において、11はプロセッサを、12はネットワークを介して計算機2と通信を行うための通信ポートを、13は電子データを保存するハードディスクやCD-R等の大容量記憶媒体を、14は主制御プログラム、ハッシュプログラム、鍵生成プログラム、暗号化プログラム、復号プログラム等の原本性保証電子保存方法を実現するためのプログラムが格納されたEEPROM、ROM等で構成されたプログラム格納媒体を、15は装置プライベートキー、装置公開鍵証明書、最新ファイル識別番号、媒体認証コードリストなどが記憶される内部記憶媒体を、16はICカード3が挿入されるICカードリーダー/ライタを、17はタイマをそれぞれ示している。

【0024】図1に示す大容量記憶媒体13としては、光磁気ディスクやCD-Rのように電子保存装置1から取り外し可能であるが、その他のブロックは電子保存装置1として物理的に一体化されており、通信ポート12を介する以外に外部からアクセスできないように構成されている。すなわち、図1に示す電子保存装置1は、各ブロックに対して直接アクセスする方法のない耐タンパ性を持った装置である。

【0025】耐タンパ性を確保するレベルとしては、電子保存装置1の筐体を開けることができないようにシールを貼る程度のものから、筐体を開けられてしまった場合には装置が動作しなくなるようなものまで考えられるが、耐タンパ性を持たせることが可能であればどのようなものであっても良い。

【0026】図1に示す電子保存装置1は、ユーザから保存要求のあったデータを大容量記憶媒体13に記録するものである。その際、後にデータの改ざんを検出できるようにするため、保存するデータに対して電子保存装置1自身の暗号鍵によりメッセージ認証子を付加する。

【0027】また、電子保存装置1は、大容量記憶媒体13に記録されているファイルのリストを作成し、それを大容量記憶媒体13に記録する処理を行う。このリストに対しても、同様にメッセージ認証子を付加する。

【0028】また、大容量記憶媒体13の不正なすり替えを検出するために、大容量記憶媒体13に記録されている保存ファイルリストと、それに付加されたメッセージ認証子を検出することで媒体の認証を行う。また、ファイルの作成日などに不正ができないよう、電子保存装置1に内蔵されているタイマ17から現在時刻を取得し、ファイルの属性情報として管理する。

【0029】さらに、電子保存装置1内部で、オリジナルとコピーとを区別できるように、各ファイルには「仮原本」、「原本」、「謄本」といった属性を付与して管理する。属性の付与されていないファイルは「一般」ファイルと呼ぶことにする。「原本」の属性が付与されて管理されているファイルに対し、外部から複製の作成を要求すると、複製されたファイルには「謄本」という属性が付与される。

【0030】この属性コードは、他のファイル属性情報と共に、データファイルと関連付けられたファイル属性情報ファイルとして大容量記憶媒体13に記録され、データファイルと同様、メッセージ認証子を付加して外部から変更することができないように管理される。

【0031】そして、大容量記憶媒体13を取り外して外部でその属性が改ざんされたような場合には、そのファイル属性情報ファイルに付与したメッセージ認証子を検証した際にその改ざんを検出する。

【0032】また、大容量記憶媒体13の媒体識別番号およびリスト装置署名の対からなる媒体認証コードリストを上記内部記憶媒体15内に格納し、この媒体認証コードリストを用いた媒体認証をおこなうことにより、大容量記憶媒体13の状態を過去の状態に戻すというような大容量記憶媒体13の不正なすり替えを検出する。

【0033】次に、前述した構成を有する電子保存装置1を用いて実行される原本性保証電子保存方法について、（1）電子データの保存処理、（2）保存ファイルリストの検証処理の順で具体的に説明する。

【0034】（1）電子データの保存処理

まず最初に、図1に示した電子保存装置1による電子データの保存処理について図2～図4を用いて説明する。図2は、図1に示した電子保存装置1による電子データの保存処理の概念を説明するための説明図であり、図3および図4は、電子保存装置1による電子データの保存処理手順を示すフローチャートである。

【0035】以下では、図3～図4のフローチャートに示す電子データ保存処理について、図2を参照しつつ具体的に説明するが、ここでは説明の便宜上、電子データを保存する時点で大容量記憶媒体13は正当であるものとする。

【0036】電子保存装置1のプロセッサ11は、通信ポート12を介して計算機2から電子データの保存要求を受けた場合、大容量記憶媒体13がマウントされているか否かを判定する(ステップS301)。ここで、大容量記憶媒体13がマウントされていないと判定した場合には(ステップS301否定)、プロセッサ11は、エラーにより電子データ保存処理を終了する。

【0037】一方、大容量記憶媒体13がマウントされていると判定した場合には(ステップS301肯定)、通信ポート12を介してユーザ側(計算機2)から、図2に示すデータ21およびファイル属性コード22を受け取る(ステップS302)。

【0038】そして、プロセッサ11は、受け取ったファイル属性コード22が「原本」または「仮原本」であるか否かを判定する(ステップS303)。ここで、ファイル属性コード22が「原本」または「仮原本」でないと判定した場合には(ステップS303否定)、プロセッサ11は、エラーにより電子データ保存処理を終了する。

【0039】一方、ファイル属性コード22が「原本」または「仮原本」であると判定した場合には(ステップS303肯定)、タイマ17から現在時刻を取得するとともに(ステップS304)、内部記憶媒体15から装置プライベートキー31、装置公開鍵証明書32および最新ファイルの識別番号を取得し(ステップS305)、最新ファイル識別番号をインクリメントして内部記憶媒体15に記録する(ステップS306)。

【0040】そして、電子データに現在時刻、タイマID、最新ファイル識別番号およびファイル属性コードを追加して図2に示す保存情報22とし(ステップS307)、この保存情報22についてのハッシュ値23を計算し(ステップS308)、計算したハッシュ値23を装置プライベートキーで暗号化して装置署名24とする(ステップS309)。

【0041】このようにして得た装置署名24および装置公開鍵証明書を保存情報22に追加して装置署名済み保存情報25とし(ステップS310)、この装置署名済み保存情報25を保存ファイルとして大容量記憶媒体13に保存する(ステップS311)。

【0042】そして、この大容量記憶媒体13から保存ファイルリスト30を取得し(ステップS312)、この保存ファイルリスト30の正当性を検証する(ステップS313～S314)。その結果、保存ファイルリスト30が正当でなければ(ステップS314否定)、エラー処理をおこない、正当であれば(ステップS314肯定)、書き込み禁止であるか否かをさらに調べる(ステップS315)。

【0043】そして、書き込み禁止であれば(ステップS315肯定)、エラー処理をおこない、書き込み禁止でなければ(ステップS315否定)、保存ファイルリ

スト30からファイルリストを取得して、先の保存ファイル26のエントリを追加し(ステップS316)、ファイルリストについてハッシュ値を計算する(ステップS317)。

【0044】そして、このハッシュ値を装置プライベートキーにより暗号化し、リスト装置署名とし(ステップS318)、このリスト装置署名および装置公開鍵証明書をファイルリストに追加して、新たな保存ファイルリスト30とし(ステップS319)、この保存ファイルリスト30を大容量記憶媒体13に記録する(ステップS320)。

【0045】その後、大容量記憶媒体13から媒体識別番号を取得し(ステップS321)、該媒体識別番号とリスト装置署名29との対を内部記憶媒体15の媒体認証コードリスト34に記録する(ステップS322)。このように、内部記憶媒体15上に媒体認証コードリスト34を記録する理由は、この媒体認証コードリスト34を用いて大容量記憶媒体13の媒体認証をおこなうためである。

【0046】上記一連の処理をおこなうことにより、電子データを大容量記憶媒体13に保存する際に、媒体識別番号およびリスト装置署名29からなる媒体認証コードリストを内部記憶媒体15に保存することができる。

【0047】なお、保存ファイルリスト30の署名が正しくとも、装着されている大容量記憶媒体13が所定のフォーマットで初期化されていない場合や、大容量記憶媒体13内の保存ファイルリスト30が最新の状態でない場合には、書き込みをおこなうことはできないが、かかる場合であっても大容量記憶媒体13からの読み出しはできるものとする。

【0048】(2)保存ファイルリストの検証処理
ところで、上記一連の処理では、大容量記憶媒体13が正当なものであることを前提としたが、大容量記憶媒体13の状態を過去の状態に戻すというような大容量記憶媒体13の不正なすり替えがおこなわれる可能性がある。このため、本実施の形態では、大容量記憶媒体13を装置本体に装着してマウント処理をおこなう際に、下記に示す保存ファイルリストの検証処理をおこなって、媒体の妥当性を検証する。

【0049】図5は、図1に示す電子保存装置1がおこなう保存ファイルリストの検証処理手順を示すフローチャートである。同図に示すように、保存ファイルリストの検証処理をおこなう際には、まず最初に大容量記憶媒体13から保存ファイルリスト30を取得し(ステップS501)、該保存ファイルリスト30のファイルリストに対してハッシュ値を計算し(ステップS502)、保存ファイルリスト30の装置公開鍵証明書からパブリックキーを取得する(ステップS503)。

【0050】そして、保存ファイルリスト30のリスト装置署名を取得し(ステップS504)、取得したリス

ト装置署名をパブリックキーで復号し（ステップS505）、復号したものがハッシュ値と一致するか否かを調べる（ステップS506）。

【0051】そして、両者が一致しない場合には（ステップS506否定）、エラー処理をおこない、両者が一致する場合には（ステップS506肯定）、大容量記憶媒体13から媒体識別番号を取得するとともに（ステップS507）、内部記憶媒体15から媒体認証コードリスト34を取得する（ステップS508）。

【0052】そして、この媒体認証コードリスト34に媒体識別番号と一致するものがあるか否かを調べ（ステップS509）、一致するものがある場合には（ステップS509肯定）、媒体認証コードリスト34内の該当するリスト装置署名と先のリスト装置署名とが一致するか否かを確認する（ステップS510）。その結果、両リスト署名が一致する場合には（ステップS510肯定）、保存リストファイルが正当であるものとみなす（ステップS511）。

【0053】なお、媒体認証コードリスト34に媒体識別番号と一致するものがない場合（ステップS509否定）または両リスト署名が一致しない場合には（ステップS510否定）、保存リストファイルが正当でないものとみなして書き込み禁止状態を保持して終了する。

【0054】上記一連の処理をおこなうことにより、大容量記憶媒体13を装置本体に装着してマウント処理をおこなう際に、保存ファイルリストの検証処理をおこなって、媒体の妥当性を検証することができる。

【0055】上述してきたように、本実施の形態では、電子データを保存する際に、媒体識別番号とリスト装置署名29との対からなる媒体認証コードリスト34を内部記録媒体15に記憶しておき、大容量記憶媒体13を装置本体に装着してマウント処理をおこなう際に、保存ファイルリストの検証処理をおこなって、媒体の妥当性を検証するよう構成したので、大容量記憶媒体の状態を過去の状態に戻すというような大容量記憶媒体の不正なすり替えを効率良く防止することができる。

【0056】ところで、契約書などでは、契約する双方が同一原本をそれぞれ保持することが多いため、上記電子データの保存処理やファイル属性コードの変更処理をおこなう際に、原本データを複数作成することもできる。たとえば、3部の原本を要求された場合には、0000123-01、0000123-02および0000123-03というように末尾に番号を追加したものをそれぞれの「原本」ファイルに付与するよう構成すれば、ファイル識別番号の先頭部のみを確認することにより、同じ電子データであることを確認することができる。

【0057】

【発明の効果】以上説明したように、請求項1の発明によれば、大容量記憶媒体に保存するファイルのリストを示すファイルリストを暗号化した署名情報並びに該大容

量記憶媒体の媒体識別情報に基づいて大容量記憶媒体の正当性を検証するよう構成したので、大容量記憶媒体の状態を過去の状態に戻すというような大容量記憶媒体の不正なすり替えを効率良く防止することができる原本性保証電子保存装置が得られるという効果を奏する。

【0058】また、請求項2の発明によれば、大容量記憶媒体に保存する保存ファイルのリストを示すファイルリストのハッシュ値を暗号化したリスト署名と、大容量記憶媒体の媒体識別情報とを対応づけた媒体認証コードリストを作成し、作成した媒体認証コードリストに基づいて大容量記憶媒体の正当性を検証するよう構成したので、この媒体認証コードリストを用いて大容量記憶媒体の正当性を効率良く検証することができる原本性保証電子保存装置が得られるという効果を奏する。

【0059】また、請求項3の発明によれば、媒体認証コードリストを前記内部記憶媒体に格納し、大容量記憶媒体を装置本体に装着する際に、この内部記憶媒体に格納された媒体認証コードリストに基づいて大容量記憶媒体の正当性を検証するよう構成したので、内部記憶媒体を有効に利用して大容量記憶媒体の正当性を効率良く検証することができる原本性保証電子保存装置が得られるという効果を奏する。

【0060】また、請求項4の発明によれば、大容量記憶媒体に保存するファイルのリストを示すファイルリストを暗号化した署名情報並びに該大容量記憶媒体の媒体識別情報に基づいて大容量記憶媒体の正当性を検証するよう構成したので、大容量記憶媒体の状態を過去の状態に戻すというような大容量記憶媒体の不正なすり替えを効率良く防止することができる原本性保証電子保存方法が得られるという効果を奏する。

【0061】また、請求項5の発明によれば、大容量記憶媒体に保存する保存ファイルのリストを示すファイルリストのハッシュ値を暗号化したリスト署名と、大容量記憶媒体の媒体識別情報とを対応づけた媒体認証コードリストを作成し、作成した媒体認証コードリストに基づいて大容量記憶媒体の正当性を検証するよう構成したので、この媒体認証コードリストを用いて大容量記憶媒体の正当性を効率良く検証することができる原本性保証電子保存方法が得られるという効果を奏する。

【0062】また、請求項6の発明によれば、媒体認証コードリストを前記内部記憶媒体に格納し、大容量記憶媒体を装置本体に装着する際に、この内部記憶媒体に格納された媒体認証コードリストに基づいて大容量記憶媒体の正当性を検証するよう構成したので、内部記憶媒体を有効に利用して大容量記憶媒体の正当性を効率良く検証することができる原本性保証電子保存方法が得られるという効果を奏する。

【0063】また、請求項7の発明に係る記録媒体は、前記請求項3～6のいずれか一つに記載された方法をコンピュータに実行させるプログラムを記録したことで、

そのプログラムが機械読み取り可能となり、これによって、請求項3～6の動作をコンピュータによって実現することができる。

【図面の簡単な説明】

【図1】 この実施の形態に係る原本性保証電子保存方法を実行する電子保存装置のブロック構成図である。

【図2】 図1に示した電子保存装置による電子データの保存処理の概念を説明するための説明図である。

【図3】 図1に示した電子保存装置による電子データの保存処理手順を示すフローチャートである。

【図4】 図1に示した電子保存装置による電子データの保存処理手順を示すフローチャートである。

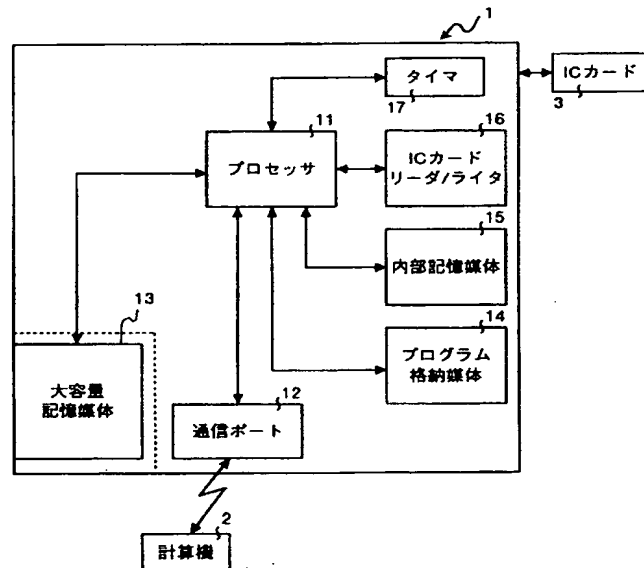
【図5】 図1に示す電子保存装置1がおこなう保存ファイルリストの検証処理手順を示すフローチャートである。

【符号の説明】

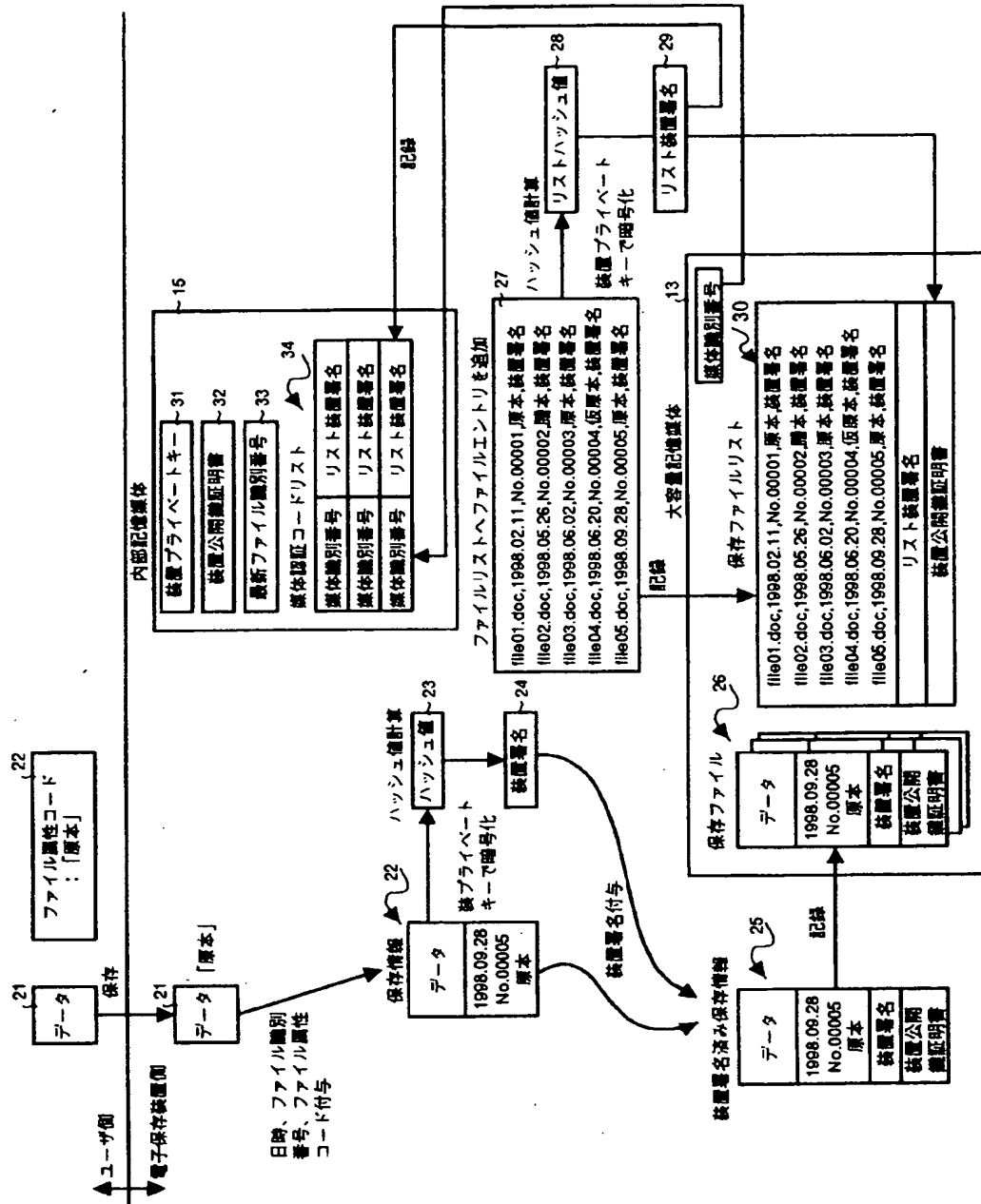
- 1 電子保存装置
- 2 計算機
- 3 ICカード
- 11 プロセッサ

- 12 通信ポート
- 13 大容量記憶媒体
- 14 プログラム格納媒体
- 15 内部記録媒体
- 16 ICカードリーダー/ライター
- 17 タイマ
- 21 データ
- 22 保存情報
- 23 ハッシュ値
- 24 装置署名
- 25 装置署名済み保存情報
- 26 保存ファイル
- 27 ファイルリスト
- 28 リストハッシュ値
- 29 リスト装置署名
- 30 保存ファイルリスト
- 31 装置プライベートキー
- 32 装置公開鍵証明書
- 33 最新ファイル識別番号
- 20 34 媒体認証コードリスト

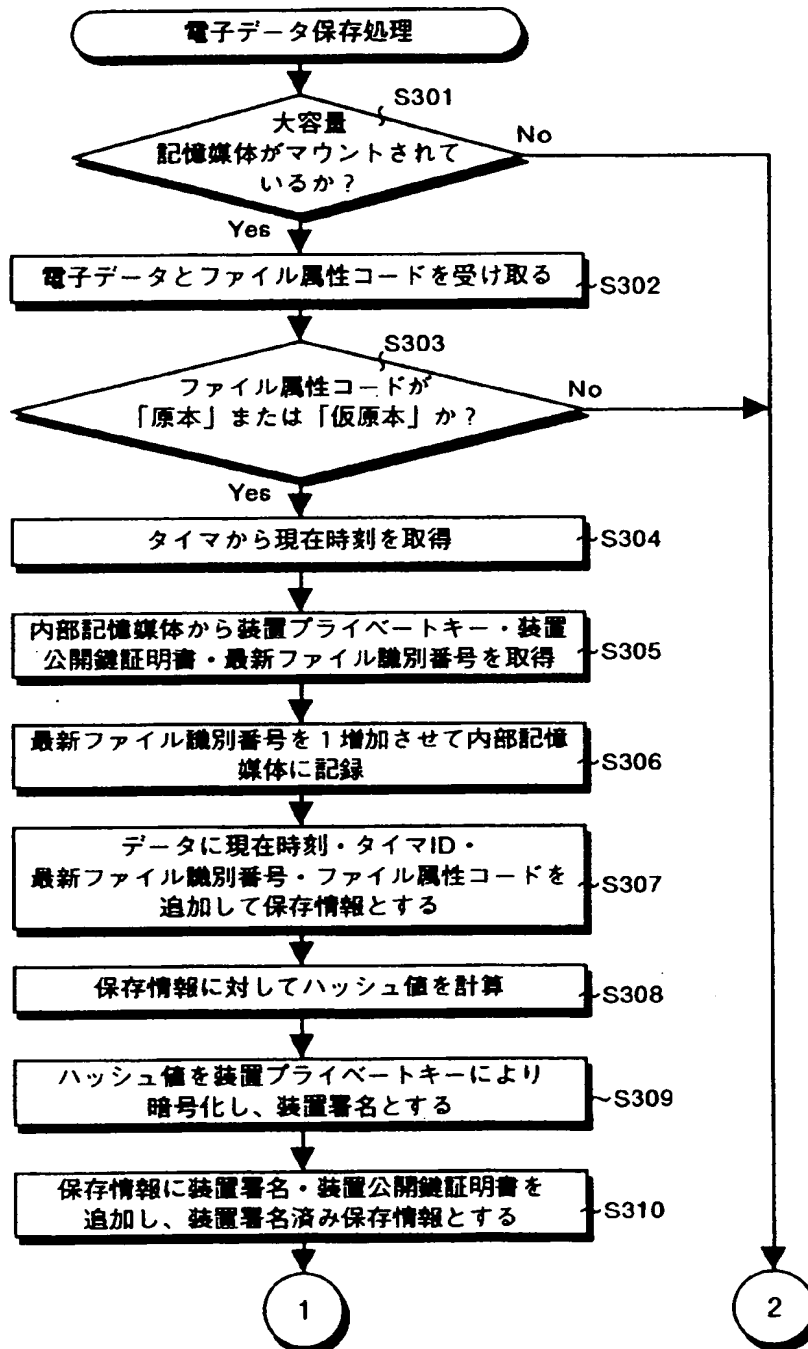
【図1】



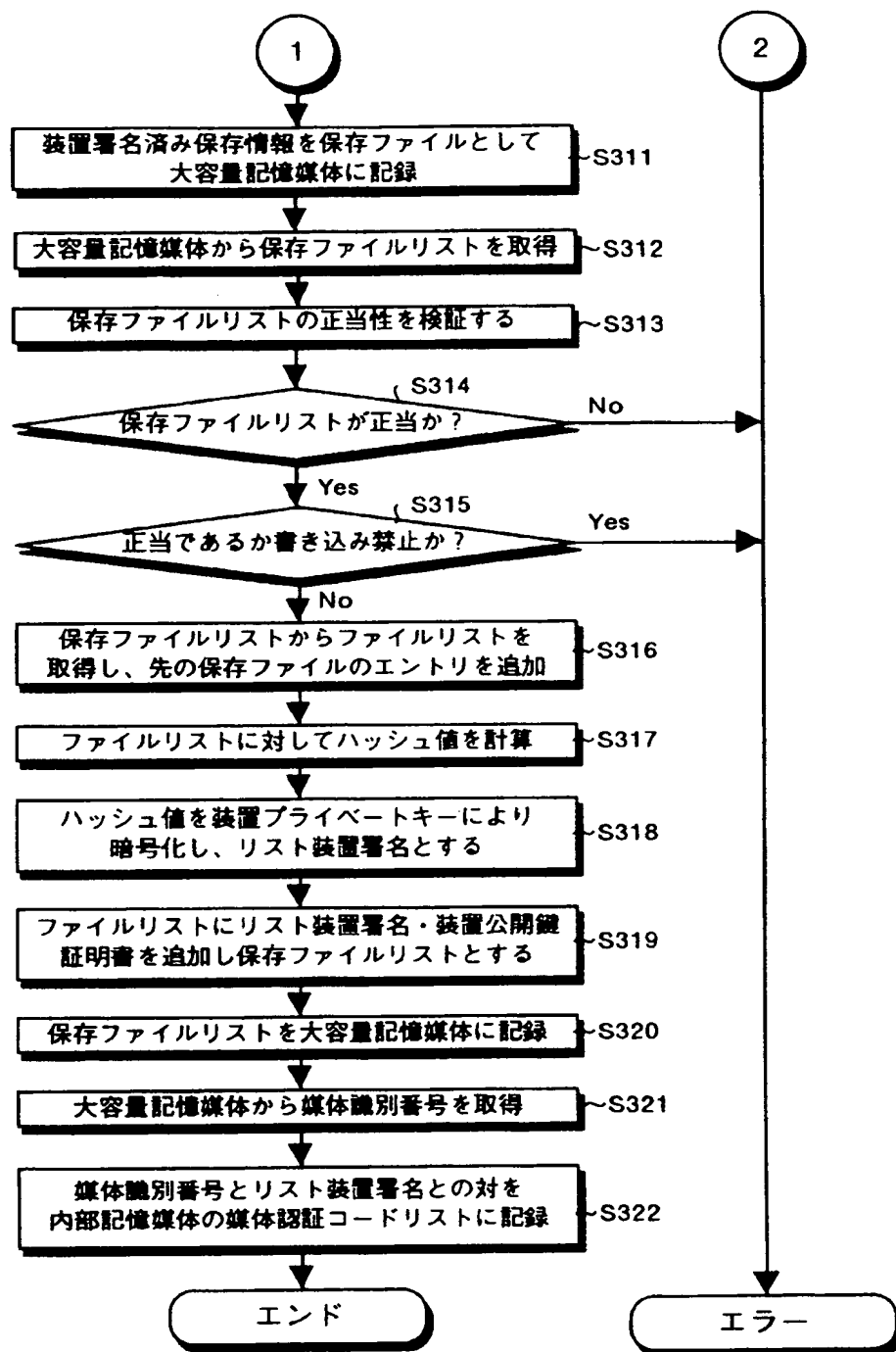
【図2】



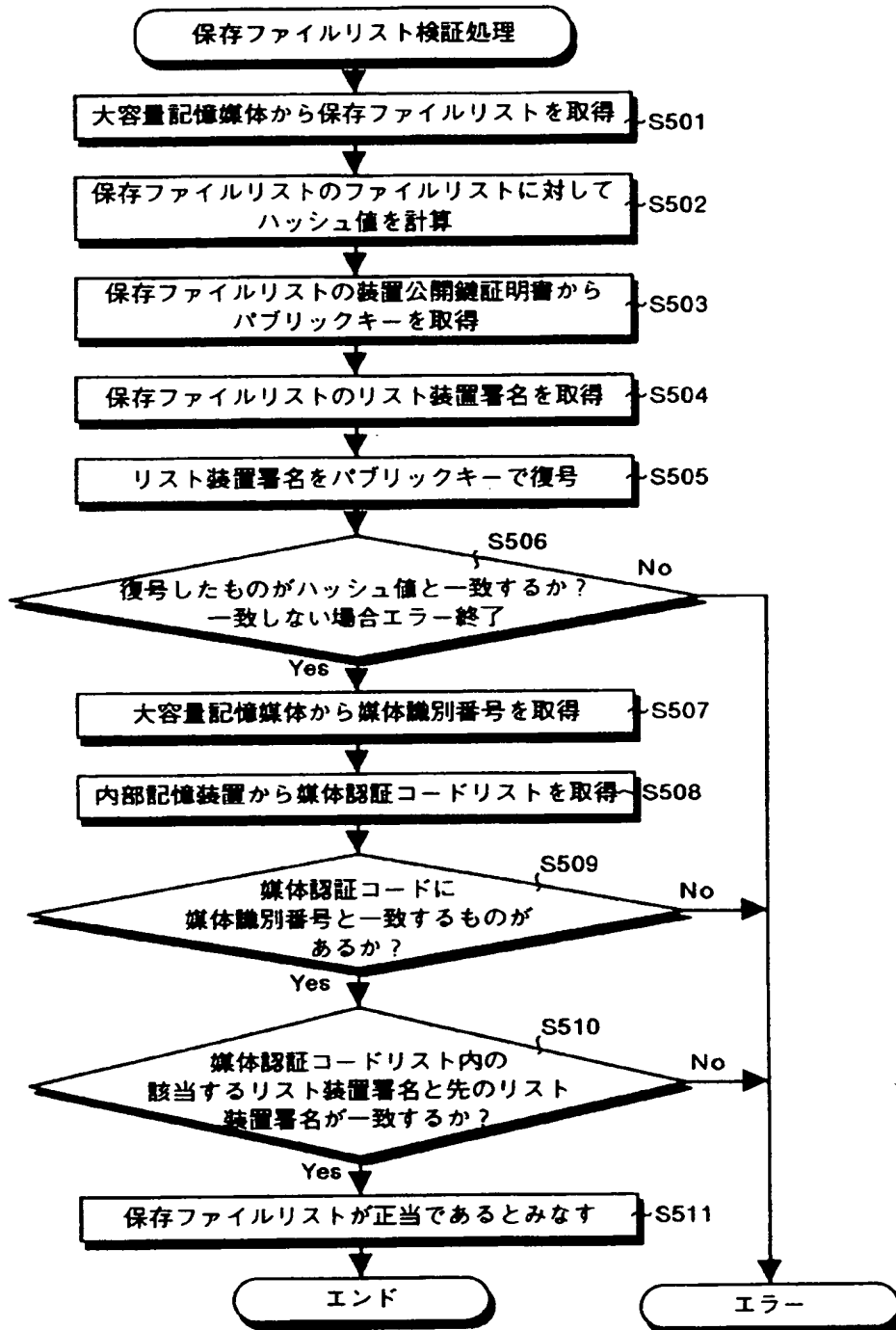
【図3】



【図4】



【図5】



フロントページの続き

F ターム(参考) 5B065 CC08 PA04 PA14 PA16 ZA04
ZA15
5J104 AA09 LA03 LA06 NA12 NA27
PA07 PA14
9A001 DD09 EE03 JJ07 LL03